System Administrators Manual (SAM) for TCP Wrappers
Version 1.0.0.2 for HP-UX 10.10
21 February 1997

1. Scope

This document provides system administrators specific guidance to support COE system and software intallation and maintenance. This document will assist system administrators in configuring the system to allow and deny access to internet services.

1.1 Identification

TCP Wrappers, Segment directory name TCPW, version number 1.0.0.2, release date 21 February, 1997. This release is for the HP/HP-UX platform operating system 10.10.

1.2 System Overview

TCP Wrappers is used to monitor and restrict network connections. By default, it logs the source and time of all network connections and attempted network connections. It can also selectively allow or deny access hosts.

2. Referenced Documents

Installation Procedures (IP) for TCP Wrappers version 1.0.0.2, 21 February 1997
`Appendix A, Unix Man Page for inetd`
`Appendix B, Unix Man Page for inetd.sec`

3. Operating Guidelines

The network services logging capability of this software logs all attempted internet services connections to the system log file, /usr/adm/syslog/syslog.log.

The default behavior of the software does not limit access to internet services. Allowing or denying internet services may be done by editing the inetd.sec file in the directory /var/adm/. To allow or deny access to a particular service, enter the following line in the inetd.sec file:

<service name> <allow|deny> <host/net address, host/net address>

Where service name is the name of a valid service in the file /etc/services, such as telnet, ftp,shell,login and host/net address is the official name or IP address of the host which you want to deny that service to. You may enter multiple host/net addresses, separated by white space. For additional information on setting up the inetd security file, see Appendix B, which is a printout of the unix man page for inetd.sec.

4. Installation Overview

Install the segment as described in the Installation Procedures Document for TCP Wrappers, version 1.0.0.2, 21 February 1997.

5. Operation/Maintenance Procedures

None.

6. Error Recovery Guidelines

If the inetd daemon needs to be restarted, it should be restarted using the -l option, which enables logging to the syslog file. If the inetd daemon is already started without logging, the superuser may issue the command inetd -l to enable logging.   When the system is booted the starts up with logging enabled. This is accomplished by setting the variable INETD_ARGS equal to “-l” in the file /etc/rc.config.d/netdaemons file. Additional information can be found in Appendix A, unix man page for inetd or Appendix B, unix man page for inetd.sec.

Appendix A. Unix Man Page for inetd

NAME Inetd(1 M)

inetd - Internet services daemon

SYNOPSIS

/usr/sbin/inetd[-c]
/usr/sbin/inetd[-k]
/usr/sbin/inetd[-l]

DESCRIPTION

The inetd daemon is the Internet superserver, which invokes Internet server processes as needed. It must be running before other hosts can connect to the local host through ftp, rcp, remsh, rlogin, and telnet. The inetd daemon also supports services based on the Remote Procedure Call (RPC) protocol (NFS), such as rwalld and rusersd. If RPC servers are started by inetd, the portmap server (see portmap(1M)) must be started before inetd.

The inetd daemon is designed to invoke all the Internet servers as needed, thus reducing load on the system. It is normally started at system boot time. Only one inetd can run at any given time.

The inetd daemon starts servers for both stream and datagram type services. For stream services, inetd listens for connection requests on Internet stream sockets. When a connection is requested for one of its sockets, inetd decides which service the socket will support, forks a process, invokes an appropriate server for the connection, and passes the connected socket to the server as stdin and stdout. Then inetd returns to listening for connection requests.

For datagram services, inetd waits for activity on Internet datagram sockets. When an incoming datagram is detected, inetd forks a process, invokes an appropriate server, and passes the socket to the server as stdin and stdout. Then inetd waits, ignoring activity on that datagram socket, until the server exits.

The inetd daemon is normally started by the /sbin/init.d/inetd script, which is invoked during the boot-time initialization. Otherwise, inetd can be started only by the superuser.

The Internet daemon and the servers it starts inherit the LANG and TZ environment variables and the umask of the process that started inetd.

If inetd is started by the superuser, it inherits the superuser's umask, and passes that umask to the servers it starts.

When invoked, inetd reads /etc/inetd.conf and configures itself to support whatever services are included in that file (see inetd.conf(4)). The inetd daemon also performs a security check if the file /var/adm/inetd.sec exists (see inetd.sec(4)). If the Internet daemon refuses a connection for security reasons, the connection is shut down. Most RPC-based services, if their first connection is refused, attempt to connect four more times at 5-second intervals before timing out. In such cases, inetd refuses the connection from the same service invocation five times. This is visible in the system log if inetd connection logging and syslogd logging for the daemon facility are both enabled (see syslogd(1M)).

The inetd daemon provides several "trivial" services internally by use of routines within itself. The services are echo, discard, chargen (character generator), daytime (human readable time), and time (machine readable time in the form of the number of seconds since midnight, January 1, 1900). The inetd daemon provides both TCP- and UDP-based servers for each of these services. See inetd.conf(4) for instructions on configuring internal servers.

Options

inetd recognizes the following options. These options can be used only by a superuser.

-c Reconfigure the Internet daemon; in other words, force the current inetd to reread /etc/inetd.conf. This option sends the signal SIGHUP to the Internet daemon that is currently running. Any configuration errors that occur during the reconfiguration are logged to the syslogd daemon facility.

-k Kill the current inetd. This option sends the signal SIGTERM to the Internet daemon that is currently running, causing it to exit gracefully. This option is the preferred method of killing inetd.

-l By default, inetd starts with connection logging disabled. If no inetd is running, the -l option causes the inetd to start with connection logging enabled. Otherwise the -l option causes inetd to send the signal SIGQUIT to the inetd that is already running, which causes it to toggle the state of connection logging.

When connection logging is enabled, the Internet daemon logs attempted connections to services. It also logs connection attempts which fail the security check. This information can be useful when trying to determine if someone is repeatedly trying to access your system from a particular remote system (in other words, trying to break into your system). Successful connection attempts are logged to the syslogd daemon facility at the info log level. Connection attempts failing the security check are logged at the notice log level. inetd also logs whether the connection logging has been enabled or disabled at the info log level.

DIAGNOSTICS

The following diagnostics are returned by the Internet daemon before it disconnects from the terminal.

An inetd is already running

An attempt was made to start an Internet daemon when one was already running. It is incorrect to call the Internet daemon a second time without the -c, -k, or -l option.

There is no inetd running

An attempt was made to reconfigure an Internet daemon when none was running.

Inetd not found

This message occurs if inetd is called with -c and another Internet daemon is running but cannot be reconfigured. This occurs if the original Internet daemon died without removing its semaphore.

Next step: Use the inetd -k command to remove the semaphore left by the previous Internet daemon; then restart the daemon.

The following diagnostics are logged to the syslogd daemon facility. Unless otherwise indicated, messages are logged at the error log level.

/etc/inetd.conf: Unusable configuration file

The Internet daemon is unable to access the configuration file /etc/inetd.conf. The error message preceding this one specifies the reason for the failure.

/etc/inetd.conf: line number: error

There is an error on the specified line in /etc/inetd.conf. The line in the configuration file is skipped. This error does not stop the Internet daemon from reading the rest of the file and configuring itself accordingly.

Next step: Fix the line with the error and reconfigure the Internet daemon by executing the inetd -c command.

system_call: message

system_call failed. See the corresponding manual entry for a description of system_call. The reason for the failure is explained in message.

Cannot configure inetd

None of the services/servers listed in the configuration file could be set up properly, due to configuration file errors.

Too many services (max n)

The number of active services listed in the configuration file exceeds the "hard" limit that can be supported by the system (see setrlimit(2)).

Next step: Reduce the number of services listed in the configuration file, then reconfigure the Internet daemon by running the command inetd -c.

file: \ found before end of line line

file can be either inetd.conf or inetd.sec. If a backslash is not immediately followed by an end of line, it is ignored and the information up to the end of line is accepted. In this case, the next line of the file is not appended to the end of the current line. Unless all the information required is present on a single line, configuration file error messages are also output. This message is logged at the warning log level.

service/protocol: Unknown service

The call to the library routine getservbyname (see getservent)) failed. The service is not listed in /etc/services.

Next step: Include that service in /etc/services or eliminate the entry for the service in /etc/inetd.conf.

service/protocol: Server failin (looping), service terminated.

When inetd tries to start 40 servers within 60 seconds for a datagram service, other than bootp, rpc, or tftp, it assumes that the server is failing to handle the connection. To avoid entering a potentially infinite loop, inetd issues this message, discards the packet requesting the socket connection, and refuses further connections for this service. After 10 minutes, inetd tries to reinstate the service, and once again accepts connections for the service.

service/protocol: socket: message
service/protocol: listen: message
service/protocol: getsockname: message

Any one of the three errors above makes the service unusable. For another host to communicate with the server host through this service, the Internet daemon needs to be reconfigured after any of these error messages.

service/protocol: bind: message

If this error occurs, the service is temporarily unusable. After 10 minutes, inetd tries again to make the service usable by binding to the Internet socket for the service.

service/protocol: Access denied to remote_host (address)

The remote host failed to pass the security test for the indicated service. This information can be useful when trying to determine if someone is repeatedly trying to access your system from a particular remote system (in other words, trying to break into your system). This message is logged at the warning log level.

service/protocol: Connection from remote_host (address)

When connection logging is enabled, this message indicates a successful connection attempt to the specified service. This message is logged at the notice log level.

service/protocol: Added service, server executable

Keeps track of the services added when reconfiguring the Internet daemon. This message is logged at the info log level.

service/protocol: New list

Lists the new user IDs, servers or executables used for the service when reconfiguring the Internet daemon. This message is logged at the info log level.

service/protocol: Deleted service

Keeps track of the services deleted when reconfiguring the Internet daemon. This message is logged at the info log level.

Security File (inetd.sec) Errors

The following errors, prefixed by /var/adm/inetd.sec:, are related to the security file inetd.sec:

Field contains other characters in addition to * for service

For example, field 2 of the Internet address 10.5*.8.7 is incorrect.

Missing low value in range for service

For example, field 2 of the Internet address 10.-5.8.7 is incorrect.

Missing highlue in ranger service

For example, field 2 of the Internet address 10.5-.8.7 is incorrect.

High value in range is lower than low value for service

For example, field 2 of the Internet address 10.5-3.8.7 is incorrect.

allow/deny field does not have a valid entry for service

The entry in the allow/deny field is not one of the keywords allow or deny. No security for this service is implemented by inetd since the line in the security file is ignored. This message is logged at the warning log level.

RPC Related Errors for NFS Users

These errors are specific to RPC-based servers:

/etc/inetd.conf: line number: Missing program number
/etc/inetd.conf: line number: Missing version number

Error on the specified line of /etc/inetd.conf. The program or version number for an RPC service is missing. This error does not stop the Internet daemon from reading the rest of the file and configuring itself accordingly. However, the service corresponding to the error message will not be configured correctly.

Next step: Fix the line with the error, then reconfigure the Internet daemon by executing the inetd -c command.

/etc/inetd.conf: line number: Invalid program number

Error on the specified line of /etc/inetd.conf. The program number for an RPC service is not a number. This error does not stop the Internet daemon from reading the rest of the file and configuring itself accordingly. However, the service corresponding to the error message will not be correctly configured.

Next step: Fix the line with the error, then reconfigure the Internet daemon by executing the inetd -c command.

AUTHOR

inetd was developed by HP and the University of California, Berkeley.
NFS was developed by Sun Microsystems, Inc.

FILES

/etc/inetd.conf	List of Internet server processes.
/var/adm/inetd.sec	Optional security file.

SEE ALSO

umask(1), portmap(1M), syslogd(1M), getservent(3N), inetd.conf(4), inetd.sec(4), protocols(4), services(4), environ(5).

Appendix B. Unix Man Page for inetd.sec

inetd.sec(4)   inetd.sec(4)

NAME

inetd.sec - optional security file for inetd

DESCRIPTION

When inetd accepts a connection from a remote system, it checks the address of the host requesting the service against the list of hosts to be allowed or denied access to the specific service (see inetd(1M)). The file inetd.sec allows the system administrator to control which hosts (or networks in general) are allowed to use the system remotely. This file constitutes an extra layer of security in addition to the normal checks done by the services. It precedes the security of the servers; that is, a server is not started by the Internet daemon unless the host requesting the service is a valid host according to inetd.sec.

If file /var/adm/inetd.sec does not exist, security is limited to that implemented by the servers. inetd.sec and the directory /var/adm should be writable only by their owners. Changes to inetd.sec apply to any subsequent connections.

Lines in inetd.sec beginning with # are comments. Comments are not allowed at the end of a line of data.

The lines in the file contain a service name, permission field, and the Internet addresses or official names of the hosts and networks allowed to use that service in the local host. The fields in each line are as follows:

```
<service name> <allow|deny> <host/net addresses, host/net names>
```

service name is the name (not alias) of a valid service in file /etc/services. The service name for RPC-based services (NFS) is the name (not alias) of a valid service in file /etc/rpc. A service name in /etc/rpc corresponds to a unique RPC program number.

allow|deny determines whether the list of remote hosts in the next field is allowed or denied access to the specified service. Multiple allow|deny lines for each service are not unsupported. If there are multiple allow|deny lines for a particular service, all but the last line are ignored.

Addresses and names are separated by white space. Any mix of addresses and names is allowed. To continue a line, terminate it with \.

Host names and network names are the official names of the hosts or networks as returned by gethostbyaddr() or getnetbynumber(), respectively. Wildcard characters (*) and range characters (-) are allowed. The * and the - can be present in any of the fields of the address. An address field is a string of characters separated by a dot (.).

EXAMPLES

Use a wildcard character to permit a whole network to communicate with the local host without having to list all the hosts in that network. For example, to allow all hosts with network addresses starting with a 10, as well as the single host with address 192.54.24.5 to use rlogin:

```
login      allow   10.*  192.54.24.5
```

On a system running NFS, deny host 192.54.24.5 access to sprayd, an RPC-based server:

```
sprayd     deny    192.54.24.5
```

A range is a field containing a - character. To deny hosts in network

10 (arpa) with subnets 3 through 5 access to remsh:

```
shell      deny    10.3-5.*
```

The following entry denies rlogin access to host cory.berkeley.edu, any hosts on the network named testlan, and the host with internet address 192.54.24.5:

```
login      deny    192.54.24.5 cory.berkeley.edu testlan
```

If a remote service is not listed in the security file, or if it is listed but it is not followed by allow or deny, all remote hosts can attempt to use it. Security is then provided by the service itself. The following lines, if present in inetd.sec, allow or deny access to the service indicated:

Allow all hosts to use ftp:

```
ftp
```

Deny all access to the shell service; i.e., remsh:

```
shell   deny
```

Allow access to the shell service by any host:

```
    shell   allow
or
    shell
```

AUTHOR

inetd.sec was developed by HP.

NFS was developed by Sun Microsystems, Inc.

FILES

/var/adm/inetd.sec

SEE ALSO

inetd(1M), gethostent(3N), getnetent(3N), hosts(4), inetd.conf(4), networks(4), protocols(4), rpc(4), services(4).